Technology in Conflict

Conflict Sensitivity for the Tech Industry

JUSTPEACE Labs

Technology in Conflict: Conflict Sensitivity for the Tech Industry

We'd like to thank Joanna Lovatt, Chloe Poynton, Helena Puig Larrauri, and Jenny Vaughan for their valuable insights and review of this publication.

Published by:

JustPeace Labs
Justpeacelabs.org
@justpeacelabs
Info [at] justpeacelabs.org

Contents

Introduction

In recent years we have increasingly seen the power of technology exploited to propagate dangerous speech, widen ethnic and religious divisions, and incite violence. Seemingly innocuous technologies now regularly contribute to human rights abuses and violent conflict. Current governance schemes are proving to be deplorably inadequate at addressing the risks of technology in conflict-affected markets. In this briefing paper, we examine the critical questions of why the technology industry should mitigate the risks of doing business in conflict-affected or high-risk areas and how it can do so.[1]

With the rapid speed and global scope of technological development, it is no surprise that technology products and services contribute to violence and conflict in diverse contexts. There is devastating evidence of how social media has been used to coordinate and direct hate-based violence in the United States[2] and to promote a terrorist attack in New Zealand.[3] Social media has also been used to further large-scale human rights abuses, armed conflict, and mass killings in places like Myanmar[4], India[5], Sri Lanka[6], and elsewhere.[7] Governments are ordering telecoms companies to shut off internet access in conflict-affected and restive areas. Advances in AI technology are being exploited as tactics in asymmetric warfare, and facial recognition is being used to repress and surveil on a mass scale. Contact tracing apps developed to fight outbreaks of COVID-19 pose serious humanitarian risks in communities where violence and tensions are on the rise. These are just the known problems with existing technology—as technology continues to develop, so will the risks and unintended consequences.

In addition to the potentially devastating loss of human life, these (mis-)uses of technology also contribute to economic stagnation and have the potential to destabilize entire regions. And when human rights abuses or conflict are linked to the involvement of a particular company or industry, that company's brand and reputation suffer. Consequently, it is in the best interest of all stakeholders, particularly the private sector, to mitigate the risks of technology being used to incite violent conflict.

"Doing business" for the tech industry raises unique considerations. The largest tech companies operate at a global scale with billions of users. This makes the scale and complexity of conflict impacts significant.

There are many ways that tech companies are inadvertently contributing to conflict dynamics. They can directly facilitate harm; incentivize harm; fail to conduct human rights due diligence; or fail to act to mitigate risks when they knew or should have known about potential harms. Sometimes technology products are used by third parties in order to foment conflict and abuse. Content moderation decisions by social media platforms can exacerbate a conflict. So can following government orders to shutdown internet services, or collect and process sensitive data. Sometimes just releasing a product or service in a conflict-affected market can have adverse impacts on the conflict. What is more, software developers are usually based in relatively insulated tech hubs in the US or Western Europe. In many cases, companies develop technology for "global" markets, and do not explicitly consider so-called "edge cases," like conflict-affected markets.

Technology's role in facilitating human rights abuse and inciting violence has become an emerging concern of regulators and civil society. They have made calls for improvements to internal and external corporate regulation. Nevertheless, the relevant domestic and international regulatory approaches remain fragmented, reactionary, and ill-equipped to respond in thoughtful and systemic ways. Moreover, most business and human rights initiatives and ethical standards fail to address many issues specific to rapidly changing technologies and their impact on human rights and conflict. They also fail to take into account how companies perceive, react to, and operationalize these norms at scale.

Many tech companies avidly support human rights and have robust internal policies for addressing issues such as privacy and free speech. However, those policies usually do not extend to conflict sensitivity or taking steps to diminish the impact of products and services on violence and conflict. There are many open questions about responsibility for harm, the impact of technology on conflict, and specific steps companies can make to support peace. Further research is urgently needed in those areas. Conflict situations present extremely high risks for companies, but attention to these issues is low. Tech companies need awareness and guidance on how to address these complex situations.

Conflict sensitivity is a tried-and-true framework for how tech companies can mitigate risks that their products and services will contribute to violence and conflict. Taking a conflict-sensitive approach to technology development has many tangible benefits for companies. It can help mitigate the legal and financial risks that arise when companies are associated with human rights abuses, violence, and armed conflict. These issues not only open up companies to civil and criminal legal liability but also negatively impact the bottom line. Early adopters of these practices can help shape emerging regulation and good practices in these areas. Finally, companies that adopt rights-aware and conflict-sensitive business practices can contribute to building peace and contributing to the UN Sustainable Development Goals.

Companies have been left with an impetus for change, but without meaningful guidance or norms for how to put that change into practice. In this briefing paper, we suggest that conflict sensitivity provides an essential framework for addressing these risks. We briefly outline some of the ways technology is contributing to conflict. We then provide a high-level overview of what conflict sensitivity is and how it relates to existing human rights frameworks. We conclude by offering recommendations for how tech companies can begin integrating conflict sensitivity into existing human rights due diligence processes.

Recommendations

The need for and benefit of conflict-sensitive business practices by the tech industry is evident. But the topic is complex, and many issues require more attention and research. Companies are grappling with difficult and nuanced questions about how best address these issues, and require detailed bespoke guidance.

We urge business leaders to incorporate a conflict sensitivity framework into their existing approaches to responsible technology. They should consider the following high-level recommendations:

1. Embrace conflict sensitivity.
2. Engage in multi-stakeholder dialogues.
3. Build internal capacity on conflict sensitivity.
4. Enhance existing human rights due diligence processes to include conflict sensitivity.
5. Conduct conflict sensitivity assessments.
6. Adopt conflict sensitivity strategies and tools.
7. Consider how different risk mitigation strategies can impact conflicts.
8. Conduct robust stakeholder engagement and community participation in high-risk markets.
9. Use community participation as a tool for stakeholder engagement.
10. Develop tools and policies to enable fast and flexible responses to emerging risks and conflicts.
11. Take advantage of opportunities to contribute to positive peace, peacebuilding efforts, and alleviating conflict drivers.

Technology in Conflict: Emerging Risks

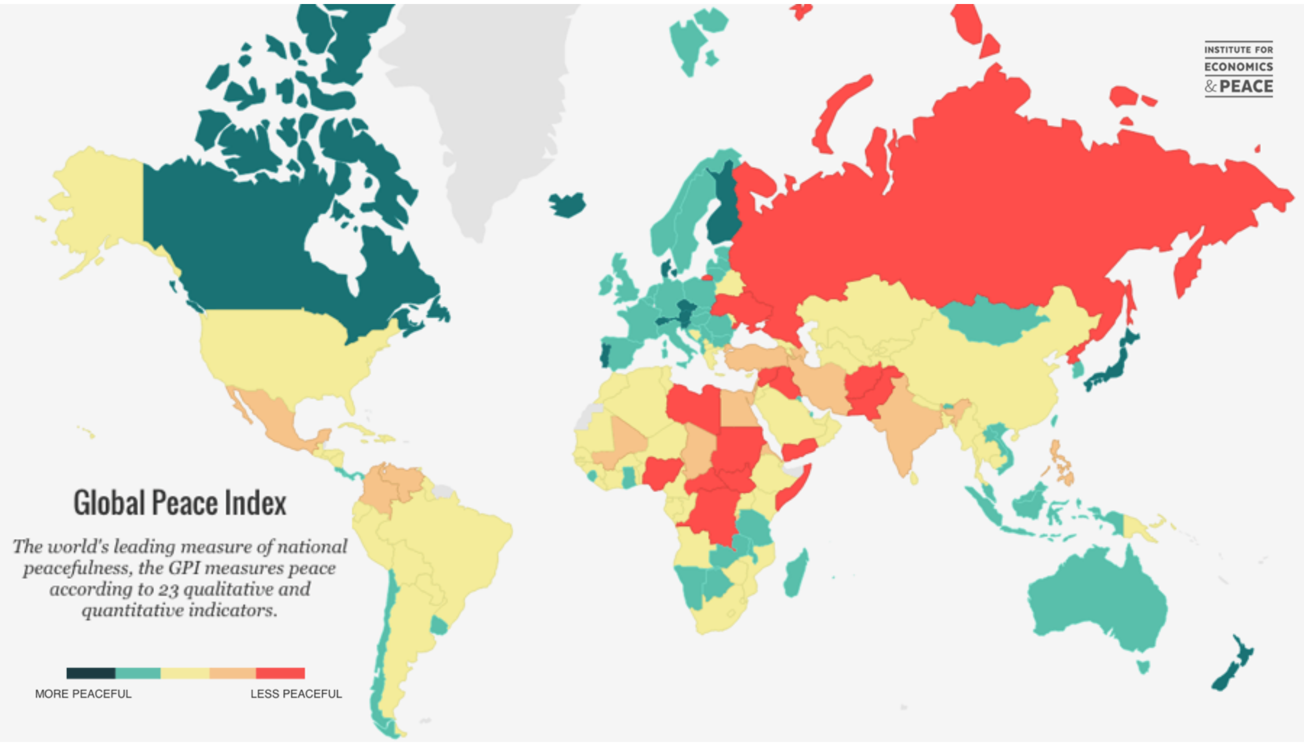
Conflict and its causes are complex topics. Put simply, conflict arises when two or more parties:

1. Believe that their interests are incompatible;
2. Express hostile attitudes towards each other; and
3. Damage the other's ability to pursue its interests.

Most of the countries in the world are experiencing some form of conflict.[8] Although this paper focuses on violent conflict, conflict does not always involve violence. Violence is just one of the many ways that parties can respond to conflict.

Conflict can occur in very diverse settings. There are many causes of conflict. Some of them include human rights or civil rights abuses; deeply-rooted community, racial or ethnic tensions; economic insecurity; or unjust governance.

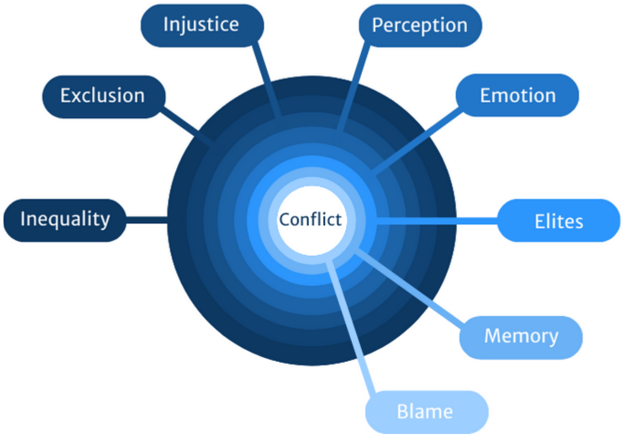
Violent conflict can lead to a severe breakdown in social relationships. It can have destructive effects on infrastructure and the economy. It can also be costly for tech companies with clients and end-users in the conflict area.


INSTITUTE FOR ECONOMICS & PEACE
Global Peace Index
The world's leading measure of national peacefulness, the GPI measures peace according to 23 qualitative and quantitative indicators.
MORE PEACEFUL
LESS PEACEFUL

Each conflict situation is highly context-specific, but a recent study by the UN and World Bank highlights common conflict drivers—root causes of violent conflict.[9] They include inequality, exclusion, and injustice. Grievances based on identity pose a particular risk. Group perceptions about these factors often matter more than actual, measurable transgressions. Objective hardships can lead to violence when enough members of a group perceive their experiences to be unjust and cast blame on another group or the state. Emotion can also contribute to mobilizing violence—fear, rage, hatred, and resentment are key emotions for violence. Collective memory and interpretations of events can be more important than the events themselves and can trigger emotional and violent reactions. These collective memories and narratives are often shaped or manipulated by powerful elites who plan and organize violence.

The risk of violent conflict is higher in areas experiencing human rights violations. Repression incentivizes violence by reinforcing the perception that citizens have no viable alternatives for expressing their grievances and frustrations.

> *"Some of the greatest risks of violence today stem from the mobilization of perceptions of exclusion and injustice, rooted in inequalities across groups. [...] When an aggrieved group assigns blame to others or to the state for its perceived economic, political, or social exclusion, then emotions, collective memories, frustration over unmet expectations, and a narrative that rouses a group to violence can all play a role in mobilization to violence." – World Bank*



Emerging technologies can significantly impact these conflict dynamics in numerous ways. The sections below provide a high-level overview of some of them.

The Weaponization of Social Media

Social media has been used to direct and coordinate mass shootings; to promote and publicize a terrorist attacks; and to incite ethnic cleansing and potential genocide. Emerging research is starting to identify common modalities for weaponizing social media to incite violent conflict around the world.[10]

Key modalities for weaponizing social media include:

1. Spreading digital hate speech;
2. Inciting violence;
3. Engaging in mis- and dis-information operations;
4. Political manipulation; and
5. Radicalization and recruitment into terrorist organizations.

These modalities appear in various contexts around the world. They impact different types of conflicts at different stages. For example, social media gives elites power and reach to manipulate perceptions about group grievances and can bring long-standing inter-communal tensions to a head, such as in Myanmar.[11] Indeed, the UN has concluded that hate speech and rumors posted on Facebook contributed to brutal crimes against Rohingya, playing a critical role in what may be a genocide.[12] It can erode social cohesion and trust by facilitating the spread of mis- or dis-information that entrenches perceived grievances and collective narratives, such as in India and South Sudan.[13] Governments weaponize it to silence opposition and incite violence, such as in the Philippines.[14] It can also play on racism or nationalism to promote racially-motivated killings or attacks, such as in the United States.[15]

Social media is a seemingly perfect weapon for spreading violence and conflict: it is cheap and has a high impact, and near-universal availability to technologically and economically weak actors. It directly impacts key conflict drivers by influencing emotions, perceptions of injustice, collective narratives, and manipulation by elites.

Indeed, some social media platforms are algorithmically designed for that. Messages that trigger strong negative emotional responses generate more attention and clicks[20]; the algorithms promote and spread posts with more attention and clicks ("reach") and those created by influencers with more followers and engagement. Fake news spreads faster than facts.[21] Neuroscience research suggests that fake news more readily grabs our attention, appeals

Case Study: Weaponization of Social Media in Sri Lanka

Sri Lanka provides an illustrative example of how social media can negatively impact fragile community relations in a complex post-conflict context. Sri Lanka has a long and complex history of inter-communal violence. Nearly a decade after the end of its 25-year civil war, many root causes of the conflict remain unaddressed. This dynamic is exacerbated by the spread of false information on social networks like Twitter, Facebook, and WhatsApp.[16]

Extremists weaponize social media to manipulate everyday people into amplifying hate speech.[17] In a country like Sri Lanka, where there is high adult literacy but extremely low digital literacy, people often trust, share, and act upon what they see on social media. Many people seem to lack an understanding of the offline effects of their online posts, message forwards, and re-tweets.

It was within this context that Sri Lanka descended into violence in 2018 as online rumors spurred deadly attacks by members of the Buddhist majority against Muslims.[18] Extremists used social media to call on people to take up arms against Muslims in response to rumors—also spread through social media—claiming that Muslims were plotting to wipe out the Buddhists.

Over the course of three days in March, mobs burned mosques, Muslim homes, and Muslim-owned shops. One man was burned to death. In response, the government temporarily blocked social media, including Facebook and two other social media platforms Facebook owns, WhatsApp and Instagram.[19]

to our emotions, and creates false memories—all related to prevalent conflict drivers.[22]

Social media has become an integral part of our communities and lives. Its prevalence, and the speed at which messages are disseminated and amplified, present serious risks for conflict.

Internet Shutdowns as Weapons of War

Internet shutdowns are increasingly common, as Governments around the world shut down internet access as a tool of oppression and a weapon of war. In 2019, 33 governments enforced 2013 internet shutdowns. Governments using internet shutdowns in the context of conflict include Sudan, Bangladesh, Ethiopia, India, and Myanmar.[23] Governments are increasingly targeting precise geographic areas, which suggests efforts to target specific populations, marginalized minority groups, and others whose human rights are at risk.[24]

Shutting down the internet blocks people from receiving essential services and information. In India, for example, the government has ordered at least 385 shutdowns since 2012. In August 2019, India imposed a complete communications blackout in Jammu and Kashmir, a region with a complex history of conflict. It had serious impacts on access to healthcare, employment, and information. It also deeply impacted the economy—Internet shutdowns in India between 2012 and 2017 reportedly cost some $3 billion in total.[29] In Myanmar, internet shutdowns have been used in conflict-sensitive areas of the country in conjunction with military offensives against armed rebel groups.[30] One shutdown in eight townships in Rakhine and Chin States has been going on for over a year. It impacts over a million people, who cannot access information, remittances, aid, or reports about outbreaks of violence and fighting. People in some villages are so cut off from news that they are unaware of the COVID-19 pandemic.[31]

AI-Driven Asymmetric Warfare

Artificial intelligence (AI) and machine learning (ML) are now being used as tactics in asymmetric warfare.[32] There are many different scenarios in which AI can be used as a weapon of war. It can expand existing threats as well as introduce new threats. Developments in AI systems will make attacks more effective, more finely targeted, and more difficult to attribute.

Case Study: Weaponization of Deepfakes in Gabon

Deepfakes are changing our assumptions about what is real and what is not. In countries with low literacy and digital literacy, experts warn that fake news and propaganda spread through faked videos could spark outbreaks of violence.[25] Falsifying videos and audio recordings allows elites to convincingly provoke emotional responses that can lead to widespread mistrust, and potentially, violent conflict.[26]

Deepfake technology has been weaponized to influence elections and harass individuals, such as investigative journalist Rana Ayyub in India.[27] In Gabon, in central Africa, an allegedly deepfake video of the President was used as justification for a military coup.[28] The video in question, released after widespread speculation that the President was ill or dead, was not fake. But the mere idea that the video was faked was enough to unravel an already precarious situation.

As AI becomes more widely available, scalable, easier to use, and cheaper, more actors will be able to use it to carry out attacks.[33]

Many potential uses of AI for conflict are still hypothetical, but it is considered one of the biggest threats for 2020.[34] Some bad actors will use AI technology in various ways to play on emotions, perceptions of grievances such as inequality, exclusion, and injustice, and create collective meaning and narratives around those issues that can erode trust and spark violent confrontations. These uses of technology closely relate to, but are not limited by, the weaponization of social media. They employ increasingly sophisticated techniques specifically intended to divide communities and instigate violence.

In one study, the Brookings Institution highlighted three particularly dangerous uses of AI as a tactic of asymmetric warfare.[35] First, they warn about advances in deep learning (a subset of machine learning).[36] These advances make it relatively easy and cheap to create dynamic disinformation videos and audio recordings and "deepfakes"—video/audio recordings that are almost imperceptibly doctored or faked using artificial intelligence. Such videos and audio recordings are difficult to detect and counteract, as they are often shared widely via platforms with end-to-end encryption. Moreover, debunking or attempting to attribute this content is often expensive compared to the cost of production, and it is challenging to get ahead of a disinformation campaign. Once mis- or disinformation is seen or heard and believed, it is very difficult to refute.

Although deepfakes can directly contribute to violence and political destabilization, it is the *awareness* of deepfakes that currently poses the biggest threat. Knowing that deepfakes are out there can undermine the perceived objectivity of real videos that feature politicians or public figures. Suddenly, humans can no longer rely on their power of perception to form opinions and understand facts.

Secondly, Brookings notes the risks caused by advances in affective computing (software that uses AI to detect and understand human emotion) and natural language processing (a form of AI that extracts meaning from human language to make decisions based on the information). These technologies—often found in "smart" devices, chatbots, customer service programs, etc.—can be weaponized to manipulate human emotions and extract sensitive information. As AI algorithms increasingly have access to personal information, it will be easier to customize these technologies, increase their appeal to users, and drive people to violence.

Third, there is a significant risk stemming from advances in content distribution networks, making it easier to reach highly specific targets with deepfakes and other emotionally manipulative content. A set of interconnected tools and services, such as data collection, digital advertising, and search engine optimization—all bolstered by advances in AI—gives rise to what is known as "precision propaganda."[37] It allows for the hyper-targeting of communications that reach millions of users with personalized messages. These tools can be used to track social attitudes in hyper-local contexts, generate customized messaging, and almost instantaneously launch personalized campaigns to manipulate behavior.[38]

These three threat vectors work together to allow for low-cost, highly effective asymmetric warfare tactics. Convincing, emotionally manipulative, and extremely targeted, they can destabilize and polarize communities and mobilize people to violence on a faster and broader scale than ever before.

Facial Recognition and Surveillance

The unregulated use of AI and facial recognition software as part of mass surveillance programs is another potential conflict driver. Machine learning now allows governments, companies, and other organizations to sort, label, and analyze vast amounts of data. Governments and other bad actors use facial recognition software built on that software to engage in mass surveillance. Widespread surveillance leads to categorical discrimination, detention, and increased social inequalities of ethnic and political minorities. It can also undermine social values and erode trust in society. These kinds of pervasive human rights abuses and social grievances are often underlying drivers for violent conflict.

Facial recognition technology can negatively impact privacy, security, and access to social services.[45] It is notoriously inaccurate, frequently misidentifying women,[46] minorities,[47] and transgender people.[48] It institutionalizes systemic discrimination and racism. For example, in the United States, police use of facial recognition technology unfairly targets

Case Study: Facial Recognition, AI, and Repression in China

In China, the government uses AI and facial recognition technology to surveil some 11 million ethnic Uyghurs and other Turkic Muslims in Xinjiang.[39] A mobile app used by police and other officials, the Integrated Joint Operations Platform (IJOP), is one of the main tools for mass surveillance and minority identification in Xinjiang. The tool monitors extreme details about individuals—including their height, hair color, personal relationships, religious speech, donations and spending, electricity consumption, whether they use the front door, socialization with neighbors—to evaluate whether a person is "normal." When the app detects irregularities or deviations from what authorities consider "normal" behavior, it generates a flag that prompts an investigation.

Human Rights Watch found that "Depending on the level of threat authorities perceive—determined by factors programmed into the IJOP system—, individuals' freedom of movement is restricted to different degrees. Some are held captive in Xinjiang's prisons and political education camps; others are subjected to house arrest, not allowed to leave their registered locales, not allowed to enter public places, or not allowed to leave China."[40]

The use of IJOP has made it easier for Chinese authorities to detain Turkic Muslims in Xinjiang arbitrarily and indefinitely on a mass scale.[41] Detainees have no rights to legal counsel, and some are subjected to torture and mistreatment, Human Rights Watch has found.[42]

What is more, the same Chinese companies that are enabling this mass surveillance of ethnic minorities in China are also exporting this technology to other, illiberal, governments. A *Wall Street Journal* report found that employees of Chinese tech giant Huawei used the company's technology to help government officials spy on political opponents in Uganda and Zambia.[43] According to the Carnegie Endowment for International Peace, Huawei has provided AI surveillance technology to at least fifty countries worldwide.[44]

Black Americans.[49] The Detroit Police reported that its facial recognition software produced a 96% error rate—yet it has relied on that software to make arrests.[50] It is increasingly being used to target, repress, and abuse political dissidents, opponents,[51] and minority groups. The risks of bias are so strong, in fact, that many top makers of facial recognition technology have paused or altogether stopped development of those products until stronger regulations are in place.[52]

Facial recognition software has been widely adopted globally for surveillance purposes, including in a significant percentage of autocratic states and illiberal democracies.[53] The Carnegie Endowment for International Peace found that "some autocratic governments—for example, China, Russia, Saudi Arabia—are exploiting AI technology for mass surveillance purposes. Other governments with dismal human rights records are exploiting AI surveillance in more limited ways to reinforce repression."[54] In some countries, like India, the technology is adopted without a corresponding data protection or electronic surveillance regulatory framework.[55]

COVID-19 and Contact Tracing

With the outbreak of the COVID-19 global pandemic, new digital threats and risks for technology to exacerbate violent conflict emerged. In response to the pandemic, governments all over the world ordered people to stay at home and started to look for ways to stop the virus from spreading. Many communities experienced an uptick in violence due to COVID-19 policy responses and flaring tensions exacerbated by increases in food insecurity, job losses, and other legitimate grievances.[56]

One established method for stemming viral infections is contact tracing. It is traditionally done manually. It is time consuming and challenging to scale up to the needs facing the world in response to the COVID0-19 pandemic. To hasten the ability to use contact tracing to track and fight outbreaks, governments and private companies partnered to develop new technology tools.

Most of these tools use location tracking or proximity tracking to identify when a user has been near another user who has been diagnosed with COVID-19. This is used to understand where outbreaks start and how they spread, and can be used to quarantine those who have come into contact with infected people.

> *The "unsuitable design or usage of [contact tracing] apps could lead to stigmatization, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity of certain populations." – ICRC.*

The effectiveness of these apps is still uncertain, especially for communities where smart-phone penetration is low. But what is certain is that in high-risk and conflict contexts, they pose a number of serious risks. A significant concern is that data collected for contact tracing can be combined with other data sets to identify and profile individuals. This could lead to or exacerbate mass surveillance and have severe humanitarian consequences. The ICRC warns that the "unsuitable design or usage of such apps could lead to stigmatization, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity of certain populations."[57]

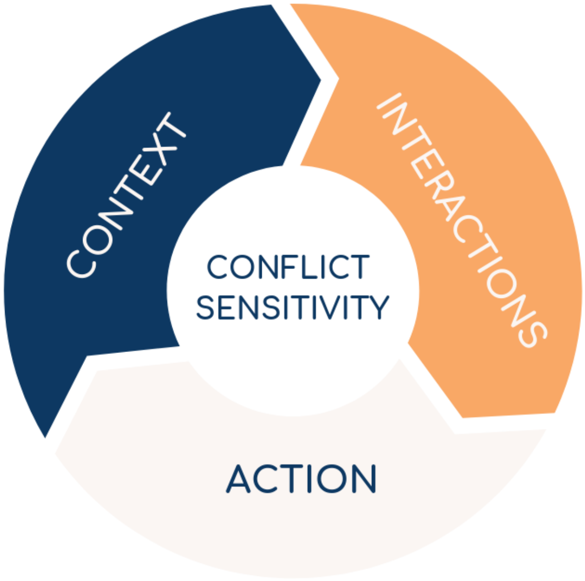
Conflict Sensitivity for Tech Companies

Conflict situations present extremely high risks for companies, but attention to these issues is low. There are many open questions about responsibility for harm, the impact of technology on conflict, and what concrete actions companies can take to support peace. Tech companies need awareness and guidance on how to address these complex situations. Many tech companies avidly support human rights and have robust internal policies for addressing issues such as privacy and free speech. However, those policies do not extend to conflict sensitivity or taking steps to diminish the impact of their products and services on violence and conflict.

Fortunately, there is a conceptual framework and developing set of tools that can help companies navigate the complexities of doing business in conflict-affected areas. Conflict sensitivity is a longstanding, tried-and-true framework that enables companies to operate responsibly and mitigate the risk that their business operations might contribute to conflict. Conflict sensitivity has increasingly been applied by diverse private industries and is now a central aspect of the UN Global Compact.[58]

On a very high level, to be "conflict-sensitive," a company should be able to:

1. Understand the context in which it operates;
2. Understand the interaction between its activities and that context;
3. Take steps to minimize the negative impacts of its operations; and
4. Take steps to maximize the positive effects of its operations for peace.



The context of a conflict is complex, dynamic, and can change quickly. It is also influenced by a company's presence in a conflict-affected market. Business operations and conflict tend to interact within a cyclical, 2-way dynamic by adversely impacting each other.

Companies offering products and services in conflict-contexts are conflict actors, even if unintentionally. The risk of becoming a major actor in a conflict is exceptionally high for tech companies, given the prevalence and importance of technology in our communications, economies, and everyday lives. Companies therefore must understand how to mitigate their effect on conflict drivers.

The pervasive nature of technology makes it nearly impossible for tech companies to avoid impacting conflicts. States, citizens, armed groups, and civil society will naturally turn to technology to further their interests and causes. Technology, including who can access it, impacts interactions between users. Companies must understand how that happens and what they can do to mitigate harmful consequences.

Conflict-affected markets are unpredictable and can evolve rapidly. And technology evolves just as quickly. Tech companies operating in these contexts must be agile enough to adjust to unforeseen changes, assess dynamic contexts, and act quickly to mitigate the risk of exacerbating the conflict.

When it comes to conflict sensitivity, technology companies face unique challenges, such as complexity and scale. Technology companies have to carefully balance seemingly competing rights, such as the right to life and the right to freedom of expression. In some situations, such as with internet shutdowns, telecom companies need to balance potential complicity in human rights abuses and conflict against violating a government order that is legal under local laws.[59] A careful, nuanced context analysis also takes time. Decisions need to be made quickly, across multiple teams, and can have far-reaching impacts beyond the relevant high-risk market. Any decision they make is likely to impact millions of people.

Effectively all of the literature, frameworks and company guides for integrating conflict sensitivity into business operations seem to refer exclusively to traditional business models. Most are written in a way that makes them effectively inapplicable to the tech industry.

Location and proximity are also challenging. While policy officers and engineers can work through a number of futures or consequence-scanning exercises, they are almost always far removed physically and experientially from conflict contexts. Properly understanding a conflict context requires specialized competence and nuanced thinking. It also requires regular engagement with local communities and civil society. But it can be challenging to establish relationships and mutual trust with local civil society groups and local experts who can help with a contextual analysis.

The good news is that the tech industry has an inherent capacity for adaptability and flexibility and is particularly well-positioned to adopt conflict-sensitive business practices. Industry leaders are accustomed to accelerating development, pivoting, and disruption in response to rapidly evolving markets and technologies. Many tech companies already have human rights policies and due diligence protocols that can be enhanced to include conflict sensitivity.

Power in Collaboration

Industry collaboration has proven a successful approach to dealing with conflict contexts for other markets. The technology industry should mirror these efforts and come together to share resources and ideas on best practices for conflict sensitivity.

Multi-stakeholder processes, built on trust and partnerships between private companies, civil society, academia, and governments, have played an important role in mitigating the risks of doing business in conflict settings in the extractive industry, diamond mining, and for companies that have private security operations. The same could be a powerful tool for the technology industry.

Together, tech companies can come together to share the burden of conflict sensitivity analysis and capacity development. For example, they could collaborate on assessing and monitoring conflict dynamics, establish fora that facilitate the exchange of relevant, non-sensitive information with civil society, and start to build trusted networks to inform their practices in high-risk markets. Sharing the burden makes it easier, faster, and more efficient to be responsive to emerging risks and conflict situations.

Human Rights and Conflict Sensitivity

Although distinct, conflict sensitivity and human rights are complementary. Human rights abuses and perceptions of injustice, exclusion, and inequality are key risk factors for violent conflict. Existing and emerging technology exacerbates these grievances. In the absence of effective and coherent regulatory frameworks, it is up to technology companies to minimize the risk that their products contribute to violent conflict. Companies that want to adopt conflict-sensitive business practices can build upon existing human rights protocols.

The UN Guiding Principles on Business and Human Rights require that companies respect all internationally recognized human rights.[60] "Respect" is twofold. First, companies must avoid directly causing or contributing to adverse human rights impacts. Second, they must take steps "to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[61] Companies must both produce and comply with meaningful human rights policies and engage in affirmative human rights due diligence practices.[62]

According to the UNGP's Principals 17 - 21, companies should:

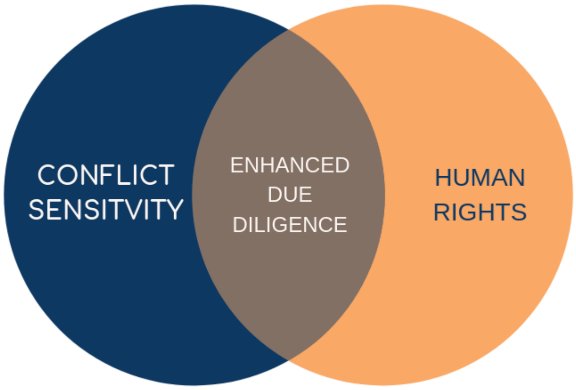
1. Assess actual and potential human rights impacts;
2. Integrate and act upon the findings;
3. Track responses; and
4. Communicate how impacts are addressed.

In line with the guidance of the UNGPs, many major companies now complete HRIAs for their high-risk supply chains or countries of operation.

There is a growing recognition that technology companies have increasingly significant impacts on human rights around the world and that the technology industry has unique considerations for how it can best respect those rights. In 2019, the UN Office of the High Commissioner for Human Rights (OHCHR) launched the B-Tech Project, which seeks to provide guidance and resources for how tech companies can better implement the UNGPs.[63] The B-Tech Project recognizes the complexities of designing corporate policy responses, acknowledging that companies must also consider complex business models, risks created by end-users, and designing accountability and remedy mechanisms at scale.

While this is a welcome advancement with respect to human rights, it does not explicitly incorporate considerations for conflict-affected markets. Many conflict situations are characterized by a history of human rights violations, weak or non-existent government regulation, and a "high risk/high gain" business culture. According to the UNGP's Guiding Principal 7, conflict-affected markets bring heightened risks for companies to become involved in human rights violations—especially severe violations. This has borne out in the emerging evidence on the weaponization of technology. Guiding Principal 7 notes that conflict-affected markets are particularly complex, and that companies' risks increase because they often lack an awareness of the political, social, and economic dynamics in those areas.

UN Guiding Principle 23 notes that the risk of being complicit in human rights abuses committed by other actors in conflict contexts is much higher and requires extra care. It recommends that companies doing business in conflict-affected markets take an "enhanced" approach to human rights due diligence.



Enhanced Human Rights Due Diligence

What does "enhanced" human rights due diligence mean in practice? Human rights due diligence and conflict sensitivity processes are complementary in many respects. Both are designed to help businesses operate responsibly and include basic impact assessment and risk mitigation techniques. However, where human rights impact assessments focus on individual rights enshrined in international law, conflict sensitivity is primarily centered on how business activities impact conflict, social cohesion, and strengthening peace. As a result, conflict sensitivity analyses tend to be more relational and contextualized.

Companies can take a series of concrete steps to include conflict sensitivity analyses into their existing human rights due diligence activities. Integrating conflict sensitivity into existing protocols is both more practical and can have more value than engaging in two separate processes.[64] This involves:

1. Conducting a detailed conflict analysis and identifying how the company's technology products and services impact the conflict;
2. Identifying ways that the company can prevent and mitigate adverse impacts on conflict and making sure that other human rights mitigation steps won't have a negative side effect on the conflict;
3. Bringing a conflict sensitivity lens and experience into human rights grievance mechanisms and community engagement programs; and
4. Protecting the safety and security of rights-holders during high risk due diligence processes.

Taking an integrated approach requires careful and balanced thinking during the assessment phase. While human rights analyses start with identifying relevant human rights, conflict sensitivity starts by considering societal dynamics. This requires an understanding of the business context and relationships between different societal groups and entails consultation with local experts and civil society organizations. There may arise situations where mitigating a potential human rights violation can worsen conflict, or where acting in a conflict-sensitive way can, at least in the short term, impede human rights. At times, being conflict-sensitive may require companies to keep impact assessments confidential if publishing it can exacerbate conflict. This may detract from transparency around important issues. An integrated approach will make these dilemmas come to light and help companies develop sound policies and procedures for navigating these complexities.

Undertaking enhanced due diligence also requires additional protections for individuals contacted during the due diligence work. These often include human rights defenders, political activists, journalists, and others who occupy contested digital spaces. Being involved in due diligence processes could put them at risk of surveillance, arrest, detention, or other forms of abuse. Moreover, companies need to ensure that rights-holders are able to safely express their views, even when they are critical of company or government practices, without fear of reprisals.

The United Nations Global Compact offers a relevant and highly practical Business Guide to Conflict Impact Assessment and Risk Management that seeks to ensure conflict sensitivity at both the pre-operational and operational stages of investment.[65] The Guide contains specific questions for businesses to answer before they enter and as they continue to operate in conflict-sensitive markets. Each question touches on a particular risk factor that can or is likely to contribute to conflict.

However, effectively all of the literature, frameworks, and company guides for integrating conflict sensitivity into business operations seem to refer exclusively to traditional business models (i.e., supply chain operations, the production of tangible goods, or the extractives industry). Most are written in a way that makes them effectively inapplicable to the tech industry.

A Note on Legislative and Regulatory Efforts

Legislative responses to these issues have been piecemeal, reactive, and fragmented. In the face of non-existent cross-border regulation, individual jurisdictions, including at the city-level, have been left to devise their own approaches. Developing sound legislative and regulatory responses takes much longer than developing new technology; regulators are constantly struggling to stay abreast of emerging technologies, corporate policies, and potential impacts on society. Moreover, these are global issues that ultimately need an international legislative or regulatory approach. Unfortunately, the feasibility of establishing and enforcing such an initiative is very low.

To date, none of the existing legislation (domestic or international), human rights frameworks, ethical standards or company initiatives (either internal or mulsti-stakeholder) have adopted or even taken into account conflict sensitivity as necessary to informing the design, deployment and ultimately use of these powerful and potentially dangerous technologies. Moreover, the specific rights and issues effected are complex and nuanced in nature. It is unclear, for example, that dangerous speech can be adequately governed by a legal or judicial framework in line with domestic and international protections regarding freedom of expression and due process concerns where speech is removed.

This is why industry regulation and multi-stakeholder efforts are so critical. They can help tech companies understand and mitigate conflict risks while allowing for bespoke approaches suitable for the tech industry. They distribute the cost and efforts of conflict analysis and harm mitigation.

Benefits of Conflict Sensitivity

There are significant benefits to adopting a conflict-sensitive approach to tech design, development, and deployment. These benefits significantly outweight the costs of joining multi-stakeholder processes and conducting enhanced due diligence processes.

Reduced Legal Liability

Companies can reduce legal liability by having a deep understanding of how their products and services are used in foreign markets and developing appropriately responsive governance policies and procedures. Taking a leading role in creating and enforcing standards for conflict-sensitive technology can reduce liability in the form of stakeholder lawsuits,[66] civil liability,[67] and other types of legal liability.[68]

Reputation Costs and Brand Identity

Harm to company reputation and brand identity can adversely effect customer loyalty and employee recruitment and retention. One study found that a bad company reputation can lead to an additional 10% cost per company hire.[69] Employees of major tech companies have become more vocal[70] about—and in some cases[71] have quit their jobs[72] over—their companies' work for the US Military and other governmental departments accused of serious human rights violations.[73]

Protecting the Bottom Line

In addition to the business harms caused by poor reputation, conflict increases the transactional cost of doing business. Sustainable business practices are positively correlated with above-average returns on investment. Morgan Stanley and researchers at Harvard have concluded that there is a positive relationship between corporate investment in sustainability and financial and operational performance.[74] In India, where the government regularly shuts down the internet in the conflict-affected Kashmir region, telecom operators lose about 24.5 million rupees ($350,000 USD) per hour that internet services are suspended.[75] In 2018, Facebook stock devalued 19% in one day, some $119bn, after it announced slower revenue and user growth following a string of problems, including the Cambridge Analytica scandal and a host of reports on the company's products being used to foment violence in Myanmar, Sri Lanka, and elsewhere.[76] And in 2020, an organized boycott over social media platforms' policies regarding hate speech and harassment saw major advertisers pull ads from the platforms.[77]

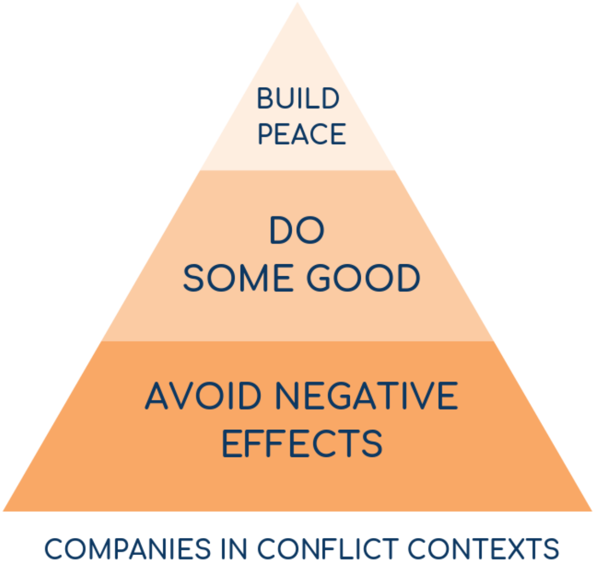
Early Adoption and Influence

It is in a company's best interest to join the development of emerging regulation and governance issues impacting its operations. Many tech companies are implicated in legal frameworks that directly conflict with their human rights commitments. There is a trend towards mandatory human rights due diligence. Civil society, advertisers, and investors are calling on tech companies to protect, not just respect, human rights. By participating in collective action and voluntary regulatory initiatives such as a multi-stakeholder initiative, companies can influence and guide the formulation of regulations and standards.

Building Peace

Effectively all major multinational companies have accepted their duty to respect human rights and the extensive responsibilities that come with that duty. Many tech companies invest heavily in human rights due diligence. Given that these companies are already spending significant resources to prevent inadvertent complicity in human rights abuses, it's only logical that they would seek to incorporate necessary conflict sensitivity provisions into these same practices to avoid inadvertently contributing to conflict. Along these lines, there are many opportunities for tech companies to support peace and actively reduce conflict drivers. Many companies today are taking positive steps in this direction.

Benefits of Adopting a Conflict Sensitive Approach



Recommendations

The need for and benefit of conflict-sensitive business practices by the tech industry is evident. But the topic is complex, and many issues require more attention and research. Companies are grappling with difficult and nuanced questions about how best address these issues, and require detailed bespoke guidance.

We urge business leaders to incorporate a conflict sensitivity framework into their existing approaches to responsible technology. They should consider the following high-level recommendations:

1. Embrace conflict sensitivity as a guiding principle throughout the design, development, and release of products and services.
2. Engage in multi-stakeholder dialogues with civil society, academia, policymakers, and other companies to develop good practices and broader understanding of conflict sensitivity and issues of responsibility, remediation, and proportionality in addressing conflict and violence.
3. Build or augment internal capacity in policy teams on human rights, conflict, and peacebuilding through new hires, training, and consultants.
4. Enhance existing human rights due diligence processes, futures planning, and ethics protocols to include comprehensive conflict sensitivity analyses.
5. Conduct conflict sensitivity assessments at each stage of design, development, and deployment of tech products, features, and services, and update them regularly.
6. Adopt conflict sensitivity strategies and tools at the product and engineering levels, such as engineer checklists, risk identification, and flagging potential harms with policy teams.
7. Consider how different risk mitigation strategies, such as pulling products or services from a high-risk market, can impact the conflict and detract from peacebuilding efforts. Develop policy guidance to enable faster, conflict-sensitive decisions on proportionality and tradeoffs between mitigating different harms.
8. Conduct robust and regular stakeholder engagement that involves civil society from high-risk markets. Be especially aware of gender considerations and the views of vulnerable and excluded groups. Ensure that rights-holders can participate without fear of reprisals or harm.
9. Use authentic and meaningful community participation as a tool for stakeholder engagement. This can, in turn, help raise awareness among communities and individuals and encourage them to provide better information on potential risks and impacts of technology in their communities.
10. Develop tools and policies to enable fast and flexible responses to emerging risks and conflicts.
11. Take advantage of opportunities to contribute to positive peace, peacebuilding efforts, and alleviating conflict drivers.

About JustPeace Labs

JustPeace Labs supports ethical and responsible approaches to technology deployed in high-risk settings. Our work advances peace and human rights protections around the world through advocacy, awareness raising, and research on effectively shaping corporate policy on conflict-sensitive tech design and development. This briefing paper is a part of our Ethics and Human Rights Program and is a companion piece to our Ethical Guidelines for PeaceTech and our Conflict Sensitivity for the Tech Industry guide. We provide strategic research, policy guidance, and analysis to diverse stakeholders who use or provide technology in high risk settings. We have engaged with tech industry stakeholders on building human rights and conflict sensitivity norms into business practices and we are actively involved with academic research and international civil society mobilization efforts to strengthen partnerships between the tech industry and civil society.

References

[1] We define “conflict-affected areas” as those regions impacted by the problems caused by ongoing or very recent conflict and the problems associated with emerging from conflict. See Håvard Strand and Marianne Dahl, “Defining Conflict-Affected Countries,” PRIO, 2010, p. 10. “High-risk area” is a region experiencing political instability or repression, institutional weakness, insecurity, weak or collapsing infrastructure, or widespread violence. Such areas are frequently characterized by widespread human rights abuses. See OECD, Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High Risk Areas, 2013, p. 13.

[2] Tim Arango, Nicholas Bogel-Burroughs, and Katie Benner, “Minutes Before El Paso Killing, Hate-Filled Manifesto Appears Online,” *New York Times*, Aug. 3, 2019.

[3] Jenni Marsh and Tara Mulholland, “How the Christchurch Terrorist Attack Was Made for Social Media,” CNN, March 16, 2019.

[4] Paul Mozur, “A Genocide Incited on Facebook, With Posts from Myanmar’s Military,” *New York Times*, Oct. 15, 2018.

[5] Soutik Biswas, “On the Frontline of India’s WhatsApp Fake News War,” BBC News, Aug. 20, 2018.

[6] Max Fisher, “Sri Lanka Blocks Social Media, Fearing More Violence,” *New York Times*, April 21, 2019.

[7] Toda Peace Institute, Social Media Impacts on Conflict Dynamics: A Synthesis of Ten Case Studies & a Peacebuilding Plan for Tech, May 2020.

[8] Vision of Humanity, Global Peace Index 2019.

[9] United Nations and World Bank Group, Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict (2018).

[10] Mercy Corps, The Weaponization of Social Media, Nov. 2019.

[11] Mozur n 4.

[12] UN Human Rights Council, Report of the detailed findings of the Independent International Fact Finding Mission on Myanmar, A/HRC/39/CRP.2, paras. 1312-1360, in particular 1342-1354 (Sept. 2018).

[13] Timothy McLaughlin, “How WhatsApp Fuels Fake News and Violence in India,” *Wired*, Dec. 12, 2018; Justin Lynch, “In South Sudan, Fake news Has Deadly Consequences,” *Slate*, June 9, 2017.

[14] Lauren Etter, “What Happens When the Government Uses Facebook as a Weapon?,” *Bloomberg Businessweek*, Dec. 7, 2017.

[15] Arango et al. n 2.

[16] Sanjana Hattotuwa, Yudhanjaya Wijeratne, and Raymond Serrato, Weaponizing 280 characters: What 200,000 tweets and 4,000 bots tell us about state of Twitter in Sri Lanka, April 23, 2018.

[17] Sanjana Hattotuwa and Yudhanjaya Wijeratne, Namal Rajapaksa, bots and trolls: New contours of digital propaganda and online discourse in Sri Lanka, Jan. 24, 2018.

[18] Amanda Taub and Max Fisher, “Where Countries are Tinderboxes and Facebook is a Match,” *New York Times*, April 21, 2018.

[19] Vindu Goel, Hari Kumar, and Sheera Frenkel, “In Sri Lanka, Facebook Contends With Shutdown After Mob Violence,” *New York Times*, March 8, 2018.

[20] Laura Hazard Owen, “One year in, Facebook’s big algorithm change has spurred an angry, Fox News-dominated — and very engaged! — News Feed,” NiemanLab, March 15, 2019.

[21] Soroush Vosoughi, Deb Roy, Sinan Aral, “The spread of true and false news online,” *Science*, March 9, 2018.

[22] Rachel Anne Barr, “Galaxy brain: The neuroscience of how fake news grabs our attention, produces false memories, and appeals to our emotions,” NiemanLab, Nov. 21, 2019.

[23] Human Rights Watch, End Internet Shutdowns to Manage COVID-19, March 31, 2020.

[24] Berhan Taye, Targeted, Cut Off, and Left in the Dark, Access Now, Feb. 2020.

[25] "Deepfake videos could 'spark' violent social unrest," *BBC News*, June 13, 2019.

[26] Clint Watts, Statement Prepared for the U.S. House of Representatives – Permanent Select Committee on Intelligence, Foreign Policy Research Institute, June 13, 2019.

[27] Drew Harwell, "Fake-porn videos are being weaponized to harass and humiliate women: 'Everybody is a potential target'," *Washington Post*, Dec. 30, 2018.

[28] Karen Hao, "The biggest threat of deepfakes isn't the deepfakes themselves," *MIT Technology Review*, Oct. 10, 2019.

[29] Rajat Kathuria, Mansi Kedia, Gangesh Varma, Kaushambi Bagchi, and Richa Sekhani, The Anatomy of an Internet Blackout, Indian Council for Research on International Economic Relations, April 2018; see also Darrell M. West, Internet Shutdowns Cost Countries $2.4 Billion Last Year, Brookings Institution, Oct. 2016.

[30] Feliz Solomon, "Internet Shutdowns Become a Favorite Tool of Governments: 'It's Like We Suddenly Went Blind,'" *Wall Street Journal*, Feb. 25, 2020.

[31] Human Rights Watch, "Myanmar: End World's Longest Internet Shutdown," June 19, 2020.

[32] Asymmetrical warfare tactics are unconventional strategies and tactics of war used by parties to conflict with less power than their opponent(s). ICRC, Asymmetric warfare.

[33] Miles Brundage et. al, General Framework for AI & Security Threats, 18.

[34] Nesta, 'Deepfake' videos get weaponized; Donie O'Sullivan, "When seeing is no longer believing," CNN, Jan. 2019.

[35] Alina Polyakova, Weapons of the weak: Russia and AI-driven asymmetric warfare, Brookings Institution, Nov. 15, 2018.

[36] Bernard Marr, "What is Deep Learning AI? A Simple Guide With 8 Practical Examples," *Forbes*, Oct. 1, 2018.

[37] Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," New America, Jan. 23, 2018.

[38] Brundage et. al n 33, 24.

[39] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019.

[40] Human Rights Watch, China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App, May 1, 2019.

[41] Megha Rajagopalan, "This is What a 21st-Century Police State Really Looks Like," BuzzFeed News, Oct. 17, 2017.

[42] Human Rights Watch, Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims, Sept. 9, 2018.

[43] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, Aug. 15, 2019.

[44] Steven Feldstein, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, Sept. 17, 2019.

[45] Access Now, Open Letter on Digital Identity Programs, Oct. 21, 2019.

[46] Steve Lohr, "Facial Recognition is Accurate, if You're a White Guy," *New York Times*, Feb. 9, 2018.

[47] Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, July 22, 2019.

[48] Os Keyes, "The Misgendering Machines: Trans/HCI Implications ofAutomatic Gender Recognition," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2, No. CSCW, Article 88 (Nov. 2018).

[49] ACLU Michigan, "Man Wrongfully Arrested because Face Recognition Can't Tell Black People Apart," June 24, 2020.

[50] Timothy B. Lee, "Detroit police chief cops to 96-percent facial recognition error rate," ArsTechnica, June 30, 2020.

[51] Joe Parkinson et al. n 43.

References

[52] Kori Hale, Amazon, Microsoft & IBM Slightly Socially Distancing From The $8 Billion Facial Recognition Market, *Forbes*, June 15, 2020.

[53] Feldstein n 44.

[54] Ibid.

[55] Rina Chandran, "Mass surveillance fears and India readies facial recognition system," Reuters, Nov. 7, 2019.

[56] Robert Muggah, David Steven, and Liv Tørres, "We urgently need major cooperation on global security in the COVID-19 era," World Economic Forum, April 23, 2020.

[57] Balthasar Staehelin and Cécile Aptel, "COVID-19 and contact tracing: a call for digital diligence," ICRC Humanitarian Law & Policy, May 13, 2020.

[58] UN Global Compact, "Peace."

[59] Solomon n 30.

[60] UN, UN Guiding Principles on Business and Human Rights (2011).

[61] UN Guiding Principles on Business and Human Rights, Principle 13.

[62] UN Guiding Principles on Business and Human Rights, Principle 15.

[63] UN Human Rights Office of the High Commissioner, B-Tech Project.

[64] Andreas Graf and Andrea Iff, "Respecting Human Rights in Conflict Regions: How to Avoid the 'Conflict Spiral'," 2 *Business and Human Rights Journal* 1, 109 (2017).

[65] Randy Gossen, Nexen Mendes, and Errol Mendes, Business Guide to Conflict Impact Assessment and Risk Management, June 2002.

[66] Shrift, Human Rights Reporting: Are Companies telling investors what they need to know?, May 2017.

[67] Nina Iacono Brown, "Should Social Networks Be Held Liable for Terrorism?," *Slate*, June 16, 2017.

[68] Ingrid Burrington, "Could Facebook Be Tried for Human-Rights Abuses?," *The Atlantic*, Dec. 20, 2017.

[69] Wade Burgess, "A Bad Reputation Costs a Company at Least 10% More Per Hire," *Harvard Business Review*, March 29, 2016.

[70] Janet Burns, "Google Employees Denounce Company's Military Drone Work In Letter to CEO," *Forbes*, Apr. 10, 2018.

[71] Janet Burns, "Google Employees Resign Over Company's Pentagon Contract, Ethical Habits," *Forbes*, May 14, 2018.

[72] Drew Harwell, "Google to drop Pentagon AI contract after employee objections to the 'business of war'," *Washington Post*, June 2, 2018.

[73] Rosalie Chan, "The Microsoft-owned Github is under pressure for its work with ICE, as employees resign and activists protest its biggest event of the year," *Business Insider*, Nov. 13, 2019.

[74] Morgan Stanley, Sustainable Reality: Analyzing Risk and Returns of Sustainable Funds, 2019; Robert G. Eccles & Ioannis Ioannou & George Serafeim, 2014. "The Impact of Corporate Sustainability on Organizational Processes and Performance," *Management Science*, vol 60(11), pages 2835-2857.

[75] Hannah Ellis-Petersen, "Many lives have been lost": five-month internet blackout plunges Kashmir into crisis," *The Guardian*, Jan. 5, 2020.

[76] Max A. Cherney, "Facebook stock drops roughly 20%, loses $120 billion in value after warning that revenue growth will take a hit," *MarketWatch*, July 26, 2018.

[77] Kim Lyons, "Coca-Cola, Microsoft, Starbucks, Target, Unilever, Verizon: all the companies pulling ads from Facebook," *The Verge*, July 2, 2020.